EXHIBIT A

2025 WL 1745726
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

KIEREN KISHNANI, Plaintiff,
v.
ROYAL CARIBBEAN CRUISES LTD., Defendant.

Case No. 25-cv-01473-NW
|
Filed 06/24/2025

ORDER GRANTING MOTION TO DISMISS

Noël Wise United States District Judge

***1** Before the Court is Defendant Royal Caribbean Cruises Ltd.'s ("Royal Caribbean") motion to dismiss Plaintiff Kieren Kishnani's first amended complaint ("FAC"). ECF No. 16. The Court GRANTS THE MOTION WITHOUT LEAVE TO AMEND.

Having considered the parties' briefs and the relevant legal authority, the Court concludes oral argument is not required, *see* N.D. Cal. Civ. L.R. 7-1(b) and VACATES the hearing set for June 25, 2025.

I. BACKGROUND

A. Factual Background

Plaintiff is a citizen of California residing in this district. See FAC ¶ 4. Royal Caribbean is a Liberian corporation that owns, operates, and/or controls www.celebritycruises.com ("Website"). *Id.* ¶ 5. Plaintiff alleges that Royal Caribbean installed "certain software on the Website designed by [third party] TikTok to seamlessly cause the extraction and transmission of data from every device that accesses the Website" ("TikTok Software"). *Id.* ¶ 11. According to Plaintiff, "each person who visits the Website can be personally identified" because the TikTok Software "fingerprint[s]" Website visitors," allowing the Website to "collect[ ] as much data as it can about an otherwise anonymous visitor to the Website." *Id.* ¶¶ 10-12. Specifically, the TikTok Software "gathers device and browser information, geographic information, referral tracking, and URL tracking by running codes or 'scripts' on the Website that send the visitor's details to TikTok." *Id.* ¶ 13. As part of Defendant's alleged use of the TikTok software, Royal Caribbean employs "Auto Advanced Matching" technology to collect further visitor information provided by the visitor to the Website. *Id.* ¶ 14. According to Plaintiff, the TikTok Software automatically runs and sends information to TikTok the moment a visitor makes a connection to the site, without visitors' consent to the tracking of their web activity. *Id.* ¶ 16.

Plaintiff contends that the TikTok software is a "trap and trace device" under the California Invasion of Privacy Act ("CIPA"). Under CIPA, a "trap and trace device" is defined as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c). According to Plaintiff, the TikTok Software is a trap and trace device because its use is to "identify the source of electronic communication by capturing incoming electronic impulses and identifying dialing, routing, addressing, and signaling information generated by users." *Id.* ¶ 18. Plaintiff alleges that the Website "is collaborating with the Chinese government to obtain [visitors'] phone number and other identifying information" without the visitors' knowledge or consent. *Id.*

CIPA imposes civil liability and statutory penalties for the installation of trap and trace devices without a court order. FAC ¶ 22; Cal. Penal Code § 638.51. Plaintiff seeks to certify a class of "[a]ll persons within California whose identifying information was sent to TikTok as a result of visiting the Website." FAC ¶ 24.

B. Procedural Background

***2** In this year alone, counsel for Plaintiff, Tauler Smith LLP, has filed at least fifteen substantively identical cases in a California federal district court. [1] Plaintiff filed the instant action February 12, 2025, and Defendant moved to dismiss on March 14, 2025. ECF Nos. 1, 11. Instead of opposing, Plaintiff filed the FAC on April 4, 2025. ECF No. 13. Defendant timely moved to dismiss on April 18, 2025. Mot., ECF No. 16.

II. LEGAL STANDARD

"In the absence of standing, a federal court lacks subject matter jurisdiction over the suit." *Righthaven LLC v. Hoehn*, 716 F.3d 1166, 1172 (9th Cir. 2013) (quotations omitted). To demonstrate Article III standing, a plaintiff must show an injury, trace that injury to the defendants' conduct, and prove that courts can provide adequate redress for the injury. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). A plaintiff must show that he suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Id.* at 560. For an injury to be particularized, it "must affect the plaintiff in a personal and individual way." *Sopeko, Inc. v. Robins*, 578 U.S. 330, 339 (2016).

"[A]n injury in law is not an injury in fact. Only those plaintiffs who have been ***concretely harmed*** by a defendant's statutory violation may sue that private defendant over that violation in federal court." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 427 (2021) (emphasis added). In other words, the legislature's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of the responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III. *Id.* In the privacy context, "[u]nless the retention of unlawfully obtained or created information amounts to the type of concrete injury recognized by the Supreme Court, it is insufficient to establish standing." *Phillips v. U.S. Customs & Border Prot.*, 74 F.4th 986, 993 (9th Cir. 2023).

As a result, general allegations of unlawful conduct are, in themselves, insufficient alone to confer standing. *Lee v. Biden*, 876 F.2d 897 (9th Cir. 1989) (citing *Allen v. Wright*, 468 U.S. 737, 754–57 (1984)); *Daghaly v. Bloomingdales.com, LLC*, No. 23-4122, 2024 WL 5134350, at *1 (9th Cir. Dec. 17, 2024) (Plaintiff fails to allege an injury in fact if he relies only on "general allegations about how [Defendant] intercepts website visitors' communications and monitors their actions" while "allegations about [Plaintiff's] own interactions with [the website] are sparse."); *see also Moore v. United Parcel Serv.*, Inc., No. 18-cv-07600-VC, 2019 WL 2172706, at *1 (N.D. Cal. May 13, 2019) ("[A] reference to invaded 'privacy and statutory rights' ... [is] insufficient to describe a concrete and particularized harm."); *Parker v. Salvation Army*, No. 20-CV-08585-JSW, 2021 WL 6618584, at *2 (N.D. Cal. Apr. 16, 2021) (same).

***3** And though in certain circumstances "[i]ntrusion on privacy alone can be a concrete injury," *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018), the nature of the injury turns on whether a plaintiff has a legitimate expectation of privacy. *Kumandan v. Google LLC*, No. 19-CV-04286-BLF, 2023 WL 8587625, at *13 (N.D. Cal. Dec. 11, 2023) (violation of CIPA requires showing "that class members had a reasonable expectation of privacy in intercepted communications."); *Rodriguez v. Autotrader.com, Inc.*, No. 2:24-CV-08735-RGK-JC, 2025 WL 1122387, at *3 (C.D. Cal. Mar. 14, 2025) ("[A]n invasion of privacy requires a reasonable expectation of privacy to have been violated.").

III. DISCUSSION

A. Plaintiff Fails to Allege an Injury in Fact

To sufficiently allege an injury in fact and "survive a motion to dismiss, a plaintiff must identify the 'specific personal information she disclosed that implicates a protectable privacy interest.' " *Khamooshi v. Politico LLC*, No. 24-CV-07836-SK,

2025 WL 1408896, at *2 (N.D. Cal. May 13, 2025) (quoting *Mikulsky v. Noom, Inc.*, 682 F. Supp. 3d 855, 864 (S.D. Cal. 2023)). Because Plaintiff did not, he lacks Standing to bring his claim. *See Hughes v. Vivint, Inc.*, No. CV 24-3081-GW-KSX, 2024 WL 5179916, at *4-5 (C.D. Cal. July 12, 2024), *adopted*, No. CV 24-3081-GW-KSX, 2024 WL 5179917 (C.D. Cal. Aug. 5, 2024) ("As Plaintiff does not clearly allege what personalized information of hers was actually collected, she does not identify any harm to her privacy."); *Mikulsky*, 682 F. Supp. at 864 (no injury in fact because "the Court is unable to determine whether the 'personal information' Plaintiff inputted is protected or whether it was merely information akin to basic contact information that would not trigger a protectable privacy interest.").

Plaintiff made four general allegations about how Defendant caused Plaintiff's alleged injury:

1) The Defendant's Website software "cause[s] the extraction and transmission of data ... so that each person who visits the Website can be personally identified." FAC ¶ 10

2) The Defendant's Website software "collects as much data as it can ... and matches it with existing data that TikTok has acquired." *Id.* ¶ 12.

3) The Defendant's Website software "gathers device and browser information, geographic information, referral tracking, and URL tracking ... ultimately sent to TikTok." *Id.* ¶ 13.

4) The Defendant's Website software "scans every page of the Website visited for additional information about the visitor, such as name, date of birth, and address." *Id.* ¶ 14.

Taken together, Plaintiff alleges only that Defendant invaded his privacy by impermissibly collecting Plaintiff's "data" and "information." A court considering a near identical complaint (*see supra* n.1) found the allegations insufficient to confer Article III standing because:

> Plaintiff fails to allege any basic facts from which the Court could infer a concrete injury, like when and how many times she visited the site, what information she provided, what information Defendant captured, whether she was aware of Defendant's tracking practices, or if she has any reason to believe that she was indeed de-anonymized.

Heiting v. FKA Distrib. Co., No. 2:24-CV-07314-HDV-AGR, 2025 WL 736594, at *3 (C.D. Cal. Feb. 3, 2025) (internal citation omitted). "Plaintiff cannot establish constitutional standing based on conclusory statements." *Steinmeyer v. Am. Ass'n of Blood Banks*, 715 F. Supp. 3d 1302, 1318 (S.D. Cal. 2024).

***4** Likewise, even if Plaintiff's allegations were sufficiently concrete and particularized (they are not), Plaintiff has failed to allege the invasion of a legally protected right. *Lujan*, 504 U.S. at 560. The mere "collection of basic contact information by ... software[,] or where the plaintiffs merely visited the website[,] are not concrete harms." *Smidga v. Spirit Airlines, Inc.*, No. 2:22-CV-1578-MJH, 2024 WL 1485853, at *4 (W.D. Pa. Apr. 5, 2024) (collecting cases); *Carolus v. Nexstar Media Inc.*, No. 24-CV-07790-VC, 2025 WL 1338193, at *1 (N.D. Cal. Apr. 9, 2025) (refusing so find an injury in fact where plaintiffs alleged only that defendant tracked "browser and device data" and "other identifying information" alongside IP addresses). IP addresses, for example, can provide "device and browser information" and "geographic information" the collection of which purportedly invaded Plaintiff's privacy in the instant case, FAC ¶ 13, but it is well established in the Ninth Circuit that "there is no legally protected privacy interest in IP addresses." *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1189 (N.D. Cal. 2020); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("Internet users have no expectation of privacy in ... the IP addresses of the websites they visit."); *Carolus*, 2025 WL 1338193, at *1 (no injury in fact where plaintiff alleges only "that a given device visited [Defendant's] website and the general location of that device, including what zip code it's in.").

And though Plaintiff alleges that Defendants *could* gain "additional information about [a] visitor such as name, date of birth, and address," and that allegation *could* intrude on Plaintiff's right to privacy, he fails to convert that hypothetical into concrete harm to *him*. FAC ¶ 14. Plaintiff does not allege that the Website collected *his* biographical information, and a "class representative must be a part of the class and ... suffer the same injury as the class members." *Falcon*, 457 U.S. at 156. A plaintiff does not have standing to bring a claim on behalf of a class if he does not have standing to bring it for himself. *Hawkins v. Comparet–Cassani*, 251 F.3d 1230, 1238 (9th Cir.2001) (citing *O'Shea*, 414 U.S. at 493–94).

Without standing, the Court is without subject matter jurisdiction. Defendant's motion is GRANTED.

B. The TikTok Software is Not a Track and Trace Device

Even if Plaintiff did allege that additional information about *him* was collected by the Website, the FAC still fails because, if that type of information is collected, the statute ceases to apply. Plaintiff's single claim turns on whether Defendant's Website and the related software constitute a "trap and trace device" as defined by Cal. Penal Code § 638.50(c) and penalized by § 638.51. By definition, a "trap and trace device" captures identifying information ***about*** a communication "***but not the contents*** of a communication." § 638.50(c) (emphasis added).

As the Superior Court of Los Angeles County explained when a substantively identical claim (*see supra* n.1) came before it:

> the crucial distinction from other devices is that ... "trap and trace devices" are designed to capture information ***about the communication***, but ***not the content of the communication*** itself. Indeed, other devices accomplish that, and a host of statutes and caselaw are directed at those other devices too. For purposes of Section 638.51, "trap and trace devices" by definition are tools which provide information about the "who," "when," and "where" of communications—but not the "what."

Price v. Headspace, Inc., No. 24STCV19921, 2025 WL 1237977, at *3 (Cal. Super. Apr. 01, 2025). The FAC alleges that the TikTok Software "fingerprint[s]" Website visitors to "collect[ ] as much data as it can about a normally [sic] and otherwise anonymous Website visitor." FAC ¶ 12. Even more intrusive, Plaintiff claims, is the "Auto Advanced Matching" technology which deploys the TikTok Software to "scan[ ] every page of the Website visited for additional information about the visitor, such as name, date of birth, and address." *Id.* ¶ 14. [2] Any "fingerprint" that reveals biographical information is "the content" of any communication between visitor and Website, [3] and thus, the claim and the case cannot survive.

* * *

5** Though neither party discusses the distinction between information ***about a communication versus information ***within*** a communication, it crystalizes the futility of Plaintiff's suit (and the myriad identical cases Plaintiff's counsel has filed in both federal and state courts). If Defendant only collects information regarding the "metadata" of the communication, Plaintiff's right to privacy is not invaded because he has no expectation of privacy as to that type of data (e.g., his IP address or general geographic location). If Defendant instead collects content information from communication between the parties (e.g., information provided from Plaintiff to Defendant directly), then the TikTok software is not a trap and trace device and § 638.50 does not apply.

For this reason, any amendment to the FAC cannot cure Plaintiff's lack of standing to bring suit. Defendant's motion is GRANTED without leave to amend. Plaintiff's FAC is dismissed with prejudice.

IT IS SO ORDERED.

All Citations

Slip Copy, 2025 WL 1745726

Footnotes

1 *See* (1) *Mitchener v. PRN Health Services, LLC*, Case No. 5:25-cv-00013 (N.D. Cal. Jan 02, 2025); (2) *Velasco v. Momentum Solar, LLC*, Case No. 2:25-cv-00016 (C.D. Cal. Jan 02, 2025); (3) *Mitchener v. New York Life Insurance Company*, Case No. 5:25-cv-00179 (N.D. Cal. Jan 06, 2025); (4) *Schallert v. Super ATV, LLC*, Case No. 2:25-cv-00108 (C.D. Cal. Jan 06, 2025); (5) *Conohan v. Rad Power Bikes, Inc.*, Case No. 2:25-cv-00106 (C.D. Cal. Jan 06, 2025); (6) *Kishnani v. Blue Nile, Inc.*, Case No. 2:25-cv-00105 (C.D. Cal. Jan 06, 2025); (7) *Schallert v. SonderMind Inc.*, Case No. 2:25-cv-00383 (C.D. Cal. Jan 15, 2025); (8) *Mitchener v. Universal Pictures Home Entertainment LLC*, Case No. 5:25-cv-00592 (N.D. Cal. Jan 16, 2025); (9) *Deol v. Z Gallerie Home LLC*, Case No. 2:25-cv-00605 (C.D. Cal. Jan 23, 2025); (10) *Hassid v. Alex and Ani, LLC*, Case No. 2:25-cv-00679 (C.D. Cal. Jan 27, 2025); (11) *Hassid v. Bohme LLC*, Case No. 2:25-cv-02492 (C.D. Cal. Mar 20, 2025); (12) *Haviland v. Avant Healthcare Professionals, LLC*, Case No. 2:25-at-00421 (E.D. Cal. Mar 31, 2025); (13) *Haviland v. Avant Healthcare Professionals, LLC*, Case No. 2:25-cv-00987 (E.D. Cal. Mar 31, 2025); (14) *Orr v. Prime Time Healthcare LLC*, Case No. 2:25-cv-02871 (C.D. Cal. Apr 02, 2025); (15) *Velasco v. Healthline Media, LLC*, Case No. 2:25-cv-02940 (C.D. Cal. Apr 03, 2025).

2 As discussed above, Plaintiff failed to allege that his "additional information" was gathered by Defendant. The analysis that follows presumes Plaintiff could allege such a thing if given leave to amend or a class member who suffered such an injury becomes lead.

3 The FAC is vague as to how a visitor's biographical information could appear on a "page of the Website" for Defendant's collection. The only circumstance the Court can conceive for such information to be available on a commercial website is that the visitor input that information himself. And if the visitor input that data, it follows that the data ***itself*** is the "content" of the visitor's communication with the Website once he provides it to Defendant.

End of Document